IN THE SPECIFICATION

Standard ANSI-41 Authentication

[0092] The standard ANSI-41 approach to producing authentication keys is depicted in Figure 3. The A-key [[300]] (which is the secret data known only to the mobile station and authentication center) and a random number called RANDSSD [[302]]are processed using a CAVE algorithm [[304]] to produce a 128-bit number called the Secret Shared Data (SSD). This operation is performed in the mobile station and the authentication center. The SSD consists of a 64-bit SSD-A key [[306]] used for authentication and a 64-bit SSD-B key used for encryption. On each system access the mobile station generates an authentication response (AUTHR) [[308]] by processing SSD-A [[306]], ESN [[310]], MIN [[312]], authentication data [[314]] (AUTH_DATA – either IMSI_S or dialed digits depending on the system access type) and a random number (RAND) [[316]] broadcast by the RAN in overhead messages. The processing is performed again by executing the CAVE algorithm [[318]]. The mobile station transmits AUTHR [[308]] in the system access and is authenticated when the authentication center (or optionally the MSC/VLR) independently performs the same computation and compares the result with that received.

Using Kc as SSD-A

KAM 9/28/07 [0092] 93

The goal of authenticating a GSM subscriber in an ANSI-41 network using the GSM authentication credentials can be achieved by using Kc as SSD-A. The new method to generate the SSD-A key and AUTHR [[402]] in accordance with an embodiment is shown in Figure 4. When the GSM authentication [[404]] is run at the mobile station and at the GSM AuC, the secret key Ki [[412]] (known only to the subscriber's SIM and the GSM AuC) and the random number (GSM_RAND) [[414]] are used to produce the SRES [[410]] and the encryption key Kc [[412]]. Kc [[412]] is 64 bits in length just as SSD-A. Therefore, Kc [[412]] can be substituted for the SSD-A value in the standard ANSI-41 computation of AUTHR using a CAVE algorithm [[416]].

KAM 9/28/07 [0094]

Since the GGG gets the GSM authentication triplets (i.e., GSM_RAND, SRES and Kc) from the GSM AuC and the RAND [[418]], ESN [[420]], MIN [[422]] and